ВЕРОЯТНОСТНЫЕ СВОЙСТВА ОЦЕНКИ МНОГОМЕРНОЙ ЭНТРОПИИ ВЫХОДНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ КРИПТОГРАФИЧЕСКИХ ГЕНЕРАТОРОВ

Палуха В. Ю., Харин Ю. С.

БГУ, НИИ прикладных проблем математики и информатики, факультет прикладной математики и информатики, Минск, Беларусь, e-mail: palukha@bsu.by, kharin@bsu.by

Для защиты информации в Интернете используются криптосистемы, неотъемлемым элементом которых являются генераторы псевдослучайных последовательностей [1]. Для оценки качества генератора предлагается вычисление статистической оценки многомерной (*s*-мерной) энтропии наблюдаемой последовательности и сравнение её с ожидаемыми свойствами оценки энтропии равномерно распределённой случайной последовательности (РРСП).

Пусть наблюдается стационарная в узком смысле двоичная последовательность $\{x_t\} \in V = \{0, 1\}$ на некотором вероятностном пространстве (Ω, F, P). Построим частотную оценку вероятности $p_J(s) = P\{X_1^s = J_1^s\}$, где $J_1^s = (j_1, \ldots, j_s) \in V_s$ – мультииндекс, по n фрагментам длины $s \geq 1$, и затем построим оценку s-мерной энтропии по «подстановочному» принципу: $\hat{h}(n, s) = -\sum_{J \in V_s} \hat{p}_J(s) \ln \hat{p}_J(s)$.

В специальной асимптотике, когда частотные оценки вероятностей s-грамм имеют Пуассоновское распределение, мы можем использовать результаты статьи [2] для доказательства следующей теоремы.

Теорема. При истинной гипотезе H_* = {{x_t} – РРСП} статистическая оценка s-мерной энтропии $\hat{h}(n, s)$, построенная по подстановочному принципу, при $n, N = 2^s \to \infty, n/N \to \lambda, 0 < \lambda < \infty$, имеет асимптотически нормальное распределение $\hat{h}(n, s) \sim \mathrm{N}(\mu, \sigma^2)$, где для параметров асимптотического распределения справедливы следующие формулы:

$$\mu = \ln n - e^{-\lambda} \sum_{k=1}^{+\infty} \frac{\ln(k+1)\lambda^k}{k!},$$

$$\sigma^2 = \frac{e^{-\lambda}}{n} \sum_{k=1}^{+\infty} \frac{(k+1)\lambda^k}{k!} \ln^2(k+1) - \frac{e^{-2\lambda}}{2^s} \left(\sum_{k=1}^{+\infty} \frac{\ln(k+1)\lambda^k}{k!} \right)^2 - \frac{e^{-2\lambda}}{n} \left(\sum_{k=1}^{+\infty} \ln(k+1) \frac{\lambda^k}{k!} (k+1-\lambda) \right)^2.$$

Полученные результаты позволяют построить решающее правило для проверки гипотез о том, является ли наблюдаемая последовательность генератора «чисто случайной»: H_* и $\overline{H_*}$. В случае принятия решения о справедливости гипотезы H_*

можно сделать вывод о том, что генератор пригоден для использования в криптосистемах.

Литература

1. Криптология / Ю.С. Харин [и др.]. – Минск: БГУ, 2013. – 512 с.